

ICS 43.040
CCS T 40



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 46194-2025

Road vehicles - Cybersecurity engineering

道路车辆 信息安全工程

(English Translation)

Issued on: October 5, 2025

Implemented on: October 5, 2025

Issued by: State Administration for Market Regulation

Table of Contents

Preface	
1 Scope	
2 Normative References	
3 Terms and Definitions, Abbreviations	
4 Overall consideration	5.
5 Organizational information security management	6.
6 Project-related information security management	
7 Distributed Information Security Activities	
8 Continuous Information Security Activities	
9 Conceptual Phase	
10 Product Development	
11 Information security confirmation	
12 Production	
13 Operation and maintenance	
14 Information security support termination and obsolescence	
15 Threat Analysis and Risk Assessment Methods	
Appendix A (Informative) Summary of Information Security Activities and Achievements	
Appendix B (Informative) Example 43 of Information Security Culture	
Appendix C (Informative) Example 44 of Information Security Interface Protocol Template	
Appendix D (Informative) Relevance of Information Security - Example of Judgment Methods and Criteria	
Appendix E (Informative) Information Security Assurance Level	
Appendix F (Informative) Criteria Affecting Ratings	
Appendix G (Informative) Attack Feasibility Rating Guidelines	
Appendix H (Informative) Application Examples of the TARA Method - Headlight Systems and Gateways	
References	

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents".

Drafting.

This document adopts ISO/SAE21434.2021 "Road Vehicle Information Security Engineering".

The following minimal editorial changes have been made to this document.

---Added an example of Threat Analysis and Risk Assessment (TARA) for automotive gateways (see Appendix H) to help standard users better understand and apply the technology.

A good understanding of the Threat Analysis and Risk Assessment (TARA) methodology.

Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents.

This document was proposed by the Ministry of Industry and Information Technology of the People's Republic of China.

This document is under the jurisdiction of the National Automotive Standardization Technical Committee (SAC/TC114).

1 Scope

This document specifies the concepts, product development, production, and operation of electronic and electrical (E/E) systems (including their components and interfaces) in road vehicles.

Engineering requirements for information security risk management during the maintenance and decommissioning phases.

This document defines a common language framework that includes information security process requirements as well as communication and management of information security risks.

This document applies to the development or improvement of E/E systems for mass-produced road vehicles, including their components and interfaces.

This document does not specify any particular technologies or solutions related to information security.

2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included.

For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies.

This document.

GB/T 34590.3-2022 Functional safety of road vehicles - Part 3: Conceptual phase (ISO 26262-3:2018, MOD) Note. The content referenced in GB/T 34590.3-2022 is not technically different from the content referenced in ISO 26262-3:2018.

3.1 Terms and Definitions

The following terms and definitions apply to this document.

3.1.1

Architectural design Recognizable representations of components (3.1.7) and their boundaries, interfaces, and interactions.

3.1.2

assets

An object that has value or contributes to value.

Note: An asset has one or more information security attributes (3.1.20), and when these information security attributes are violated, one or more hazardous scenarios may occur (3.1.22).

3.1.3

Attack feasibility

The attributes of the attack path (3.1.4) describe the ease or difficulty of successfully executing the corresponding attack activity.

3.1.4

attackpath

attack

A set of deliberate activities to achieve the threat scenario (3.1.33).

3.1.5

attacker

Individuals, groups, or organizations that execute the attack path (3.1.4).